Investigate the Security of Electric Vehicle (EV) Ecosystem Applications

Myungsoo Jun, Ryan Cryar, and Anthony Markel

National Renewable Energy Laboratory

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5T00-90388
November 2024

Investigate the Security of Electric Vehicle (EV) Ecosystem Applications

Myungsoo Jun, Ryan Cryar, and Anthony Markel

National Renewable Energy Laboratory

Suggested Citation
Jun, Myungsoo, Ryan Cryar, and Anthony Markel. 2024. *Investigate the Security of Electric Vehicle (EV) Ecosystem Applications*. Golden, CO: National Renewable Energy Laboratory. NREL/TP-5T00-90388. https://www.nrel.gov/docs/fy25osti/90388.pdf.

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5T00-90388
November 2024

National Renewable Energy Laboratory
15013 Denver West Parkway
Golden, CO 80401
303-275-3000 • www.nrel.gov

NOTICE

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Vehicle Technologies Office. The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government.

Acknowledgments

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by the U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Vehicle Technologies Office. The authors acknowledge Mr. Lee Slezak, of the Vehicle Technologies Office Grid and Infrastructure, for his role in establishing the project concept, advancing the implementation, and providing ongoing guidance. The views expressed in the article do not necessarily represent the views of the DOE or the U.S Government.

List of Acronyms

API	Application Programming Interface
ATS	App Transport Security
CNO	Charge Network Operator
DOD	U.S. Department of Defense
EV	Electric Vehicle
EVSE	Electric Vehicle Supply Equipment
HTTP	Hypertext Transfer Protocol
MAV	Mobile App Vetting
OEM	Original Equipment Manufacturer
RASP	Runtime Application Self-Protection
URL	Uniform Resource Locator

Executive Summary

Applications that run on mobile devices are critical components of the electric vehicle (EV) ecosystem, and they pose possible threat actor points of entry that could impact the trust and security of EV charging systems in the future. Mobile apps often rely on communications between cloud servers and users, thereby creating potential points of entry for cyberattacks. Although app stores, such as the Apple App Store and Google Play Store, generally test the security of apps, the cyber aspects might not be sufficient for many entities, including the U.S. Department of Defense, federal fleets, and commercial sectors. A more thorough inspection and the ability to influence developers is imminently needed. This research studies the security attributes and vulnerabilities of a sample of mobile apps that support key user functions in the EV ecosystem. The study shows that all analyzed apps have security risks, categorized as high or medium or both, and a comprehensive cybersecurity guideline for developing mobile apps is necessary.

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Description

The objective of the task is to investigate cybersecurity within the electric vehicle (EV) ecosystem, focusing on scrutinizing the security aspects of mobile applications, or apps, that are a key component of the EV ecosystem user experience. By concentrating on these mobile apps, the task seeks to assess the potential vulnerabilities and risks embedded within the larger EV framework.

1.2 Background

Apps that run on mobile devices are critical components of the EV ecosystem, and they pose possible threat actor points of entry that could impact the trust and security of EV charging systems in the future. Mobile apps often rely on application programming interfaces (APIs) to facilitate communications between cloud servers and users, thereby creating potential points of entry for cyberattacks. Security researchers, for example, discovered that they were able to remotely connect to a car using the automobile manufacturer's mobile app, showing that an original equipment manufacturer's (OEM's) mobile app can potentially be used to remotely hack into the cars that use the mobile app [1]. Although app stores, such as the Apple App Store and Google Play Store, generally test the security of apps, the cyber aspects might not be sufficient for many entities, including Department of Defense, federal fleets, and commercial sectors. A more thorough inspection and the ability to influence developers is imminently needed.

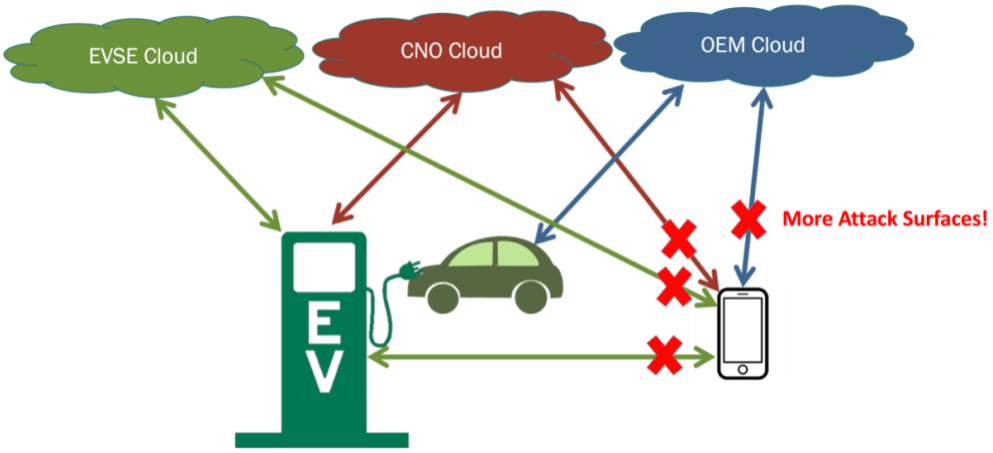

Figure 1. Mobile device in the EV ecosystem

2 Approach

First, the task conducts inventory research for the mobile apps used in the EV ecosystem that are currently available in app stores, lists the apps, and categorizes them based on an app vendor or developer. Then, the task leverages and uses a tool called Mobile App Vetting (MAV) [2], developed by the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, to assess some selected apps in the EV charging market. Thus far, five apps from charge network operators (CNOs), three from automobile manufacturers (i.e., OEMs), and two from electric vehicle supply equipment (EVSE) manufacturers have been assessed.

3 Results

MAV can be used to conduct static and dynamic code analysis to scan apps against industry standards, such as the National Institute of Standards and Technology, the National Information Assurance Partnership, the Open Worldwide Application Security Mobile Application Security Testing Guide, and Europe's General Data Protection Regulation. These standards offer detailed models for mobile app integrity by providing baseline security requirements.

Once a scan is complete, MAV findings are categorized into critical, high, medium, and low, so users can decide to deploy, remediate, or remove any app from circulation based on its established risk tolerance.

3.1 Test Results

3.1.1 Apps From Charge Network Operators

Common features of mobile apps from CNOs include:

- Find and map to an available charger.
- Receive live updates of charging status.
- Receive notifications of status or other information.
- Pay for charging.

The mobile apps need to communicate with a CNO cloud server to provide these features. Table 1 lists the risks (high and medium) identified in the CNO apps after a scan with the MAV tool.

Table 1. Summary of Security Report of CNO Apps Analyzed

Vendor	High Risk	Medium Risk
CNO A	• App Transport Security (ATS) disabled	• Loads an external library dynamically • Unencrypted network connections made • Insufficient keychain protection • Runtime Application Self-Protection (RASP) not detected • No data at rest encryption • App does not check for trusted environment
CNO B	• Uses hard-coded credentials for secure operations	• Loads an external library dynamically • Memory protections disabled • Insufficient keychain protection • RASP not detected • App does not check for trusted environment
CNO C		• Loads an external library dynamically • Insufficient keychain protection • RASP not detected • No data at rest encryption • App does not check for trusted environment
CNO D	• ATS disabled	• Loads an external library dynamically • Memory protections disabled • RASP not detected • No data at rest encryption • App does not check for trusted environment
CNO E		• Loads an external library dynamically • Does not use operating system-provided encryption • No data at rest encryption • Hypertext Transfer Protocol Uniform Resource Locators (HTTP URLs) found in app

Three of five apps have high risks, and all five apps have several medium risks. Detailed explanations of these risks are presented in Section 3.2.

3.1.2 Apps From Automobile Manufacturers

Features of the mobile apps from the OEMs include:

- View EV battery state of charge.
- Start, stop, and schedule a charging session.
- Manage charge and battery settings.
- Remotely access climate control.
- Receive notifications of vehicle-related information.

Table 2 lists the risks (high and medium) identified in the OEM apps.

Table 2. Summary of Security Report of OEM Apps Analyzed

Vendor	High Risk	Medium Risk
OEM A		• Loads an external library dynamically • Does not use operating system-provided encryption • Memory protections disabled • RASP not detected • No data at rest encryption • App does not check for trusted environment
OEM B		• Loads an external library dynamically • Memory protections disabled • Insufficient keychain protection • RASP not detected • No data at rest encryption
OEM C	• App communicates with high-risk locations	• Loads an external library dynamically • Memory protections disabled • RASP not detected • No data at rest encryption • App does not check for trusted environment

One of the three apps communicates with high-risk locations, which is considered a high risk. And all three apps have several medium risks. Detailed descriptions of these risks are presented in Section 3.2.

3.1.3 Apps From Electric Vehicle Supply Equipment Manufacturers

Common features of mobile apps from EVSE include:

- Start, stop, and schedule a charging session.
- Manage and authorize radio-frequency identification cards to be used.
- Monitor charging status in real time.
- Receive notifications.
- Remotely control charging sessions.
- Balance load.

Two apps from EVSE manufacturers were selected for analysis. Table 3 lists the risks (high and medium) identified in the EVSE apps.

None of the analyzed apps have any high risks, but the apps have several medium risks that are also identified in the apps from CNOs and OEMs. Detailed explanations of these risks are presented in Section 3.2.

Table 3. Summary of Security Report of EVSE Manufacturer Apps Analyzed

Vendor	High Risk	Medium Risk
Company A		• Loads an external library dynamically • Memory protections disabled • Insufficient keychain protection • RASP not detected • No data at rest encryption
Company B		• Loads an external library dynamically • Does not use operating system-provided encryption • Memory protections disabled • Insufficient keychain protection • RASP not detected • No data at rest encryption • App does not check for trusted environment

3.2 Results Analysis

The high risks identified in the analyzed mobile apps are:

1. App Transport Security (ATS) disabled.
2. Use of hard-coded credentials for secure operations.
3. Communication with high-risk locations.

Disabling ATS allows for the app to load resources or communicate over insecure Hypertext Transfer Protocol (HTTP) connections. These connections are vulnerable to information harvesting and man-in-the-middle attacks that could expose user and/or organizational data. The same security risk has been studied for medical mobile apps [3].

Hard-coded encryption keys are static keys that are directly embedded into the software source code and they make it difficult to rotate keys without redeploying the application. Therefore, hard-coded encryption keys allow for easy reversal of encryption operations because an attacker already has the credentials. Attackers that can locate the hard-coded key can use it to reverse any operation and gain access to the previously encrypted data. This risk applies not only to mobile apps but also to Internet of Things devices [4] and others. Dedicated key management systems instead of hard-coded encryption keys should be utilized to securely generate, store, and manage encryption keys.

Apps that connect to servers located in a country deemed high risk as determined by the list of U.S. sanctioned countries have high risks in data security. Data sent to and received in these network requests should be considered compromised due to the lack of protections and enforcement on organizations operating in these locations. This has the potential to cause a large impact on brand reputation, user trust, and general user and organizational harm from the data impacted by the requests.

The analysis also shows that all the apps selected have many medium risks. The types of risks and percentage of apps with each risk are illustrated in the graph in Figure 2.

3.2.1 Dynamic Loading of an External Library

All the analyzed apps dynamically load an external library. Dynamically loaded libraries that are not verified with a hash or other mechanism have the potential to load vulnerable and/or malicious code into the app and compromise the integrity of the app. This could lead to private information leakage of the user and/or the app development organization. If the developer does not verify the security and validity of the dynamically loaded library, it could introduce vulnerabilities, flaws, or unintended functionalities in the app.

3.2.2 No Runtime Application Self-Protection

Runtime Application Self-Protection (RASP) libraries help to secure apps against reverse engineering and other exploits on end-user devices. Approximately 90% of the analyzed apps have this risk, however. Without RASP, the app might be more vulnerable to these types of attacks. The back-end connections performed by the app may be

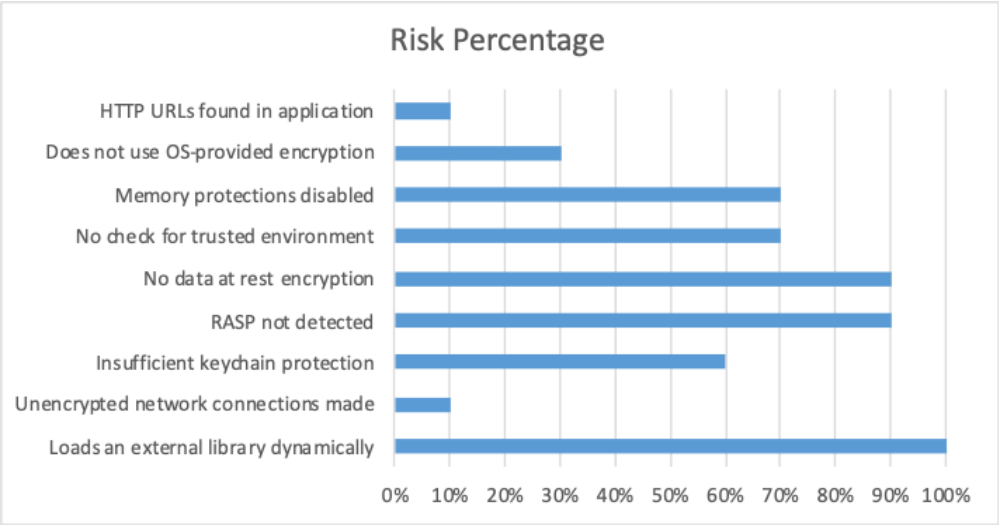

Figure 2. Statistics of medium risks of mobile apps analyzed

intercepted, monitored, or changed. This could lead to leakage of user data, unexpected app behavior, and exposure of organization sensitive data.

3.2.3 No Data at Rest Encryption

If the app handles any sensitive data, it is good practice to encrypt these data when stored locally; however, 90% of the analyzed apps do not encrypt data stored locally. If the encryption operations are not seen, it might be easier for attackers to exploit the information handled by the app; therefore, encrypting data at rest should be considered mandatory if the app is storing sensitive data on the device. Without an extra level of encryption, the data stored on the device, even in the app's private container, can be exposed if the device is compromised.

3.2.4 Not Checking for Trusted Environment

The analysis shows that 70% of the apps do not check to ensure that the operating environment can be trusted. Apps that do not check for a trusted operating environment might be vulnerable to reverse engineering and exploitation.

3.2.5 Memory Protections Disabled

Approximately 70% of the analyzed apps have disabled the built-in memory protections. Disabling the built-in memory protection can expose the app to crashes or memory exploits. The app can be unstable or unsafe to use without the memory protections enabled.

3.2.6 Insufficient Keychain Protection

The analysis indicates that 60% of the analyzed apps store data in the keychain with insufficient encryption settings. Insufficient keychain protection can allow attackers to gain easier access to data stored in the keychain. The data stored in the keychain with the insufficient encryption can be backed up to cloud services or more easily accessed by an attacker. User data and/or organization data might be at risk.

3.2.7 HTTP URLs Found in Application

Some apps (approximately 10%) contain URL(s) that specify the HTTP protocol. If any sensitive data are exchanged over the network through the app, it is essential to use encrypted network communications. If the app does not use encrypted connections, the app should not have access to any sensitive functionality or data. Encrypting data in transit should be considered mandatory if the app is sending sensitive data over the network. Without encryption, the data sent over the network can be exposed at any point between the client and the server. This can lead to data leakage and provide a view into the app and/or server operations.

4 Milestone Status and Future Directions

NREL completed an initial investigation of the security of the selected mobile apps in the EV ecosystem. The investigation revealed that there are high or/and medium security risks in all the apps that were selected for the analysis. This is only a small sample of the wide variety of mobile apps used in the EV ecosystem. Increasing the number of inventories of security assessments and analyses of common vulnerabilities and mitigation suggestions is needed for more future research to foster a safer and more secure environment for EV users, ensuring that their data and interactions remain protected.

5 Conclusions

This task studied the security attributes and vulnerabilities of a sample of mobile apps that support key user functions in the EV ecosystem. The investigation showed that all the analyzed apps have security risks, categorized as high or medium or both. A comprehensive cybersecurity guideline for developing mobile apps is needed. Continued investigation is essential to foster a safer and more secure environment for EV users, ensuring that their data and interactions remain protected. To achieve this, it is necessary to increase the number of inventories of security assessments and to analyze common vulnerabilities and mitigation strategies for further study. Future research includes:

- Extensive analysis with increased numbers of mobile apps in the market: This will provide insights into identifying common architectural vulnerabilities that app developers should address and improve to ensure security.
- Validation and verification of the identified risks by the MAV tool through hardware-in-the-loop experiments, NREL Cyber Range emulations, or dynamic analysis on captured network traffics: This can corroborate findings from MAV scans or provide other findings not from MAV scans. Additionally, it will analyze and assess the impacts on the EV charging ecosystem and suggest mitigation methods that can be executed in real-world apps.

References

[1] *Nissan Leaf Can be Hacked via Mobile App and Web Browser*, https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/nissan-leaf-can-be-hacked-via-mobile-app-and-web-browser, [Online], 2016.

[2] *Mobile Cybersecurity Shared Services*, https://www.cisa.gov/resources-tools/services/mobile-cybersecurity-shared-servicesr, [Online].

[3] G. Chatzisofroniou, C. Markellos, and P. Kotzanikolaou, "Assessing the security risks of medical mobile applications," in *2023 IEEE Symposium on Computers and Communications (ISCC)*, Los Alamitos, CA, USA: IEEE Computer Society, Jul. 2023, pp. 1–7. DOI: 10.1109/ISCC58397.2023.10217984.

[4] B. R. Chandavarkar, "Hardcoded credentials and insecure data transfer in iot: National and international status," in *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 2020, pp. 1–7. DOI: 10.1109/ICCCNT49239.2020.9225520.